

PN - JP2000216822 A 20000804
PD - 2000-08-04
PR - JP19990016634 19990126
OPD - 1999-01-26
TI - METHOD FOR ALLOCATING IP ADDRESS
IN - ONUMA TETSUYA
PA - HITACHI LTD
IC - H04L12/56 ; G06F13/00 ; G06F15/00 ; H04L12/28
© WPI / DERWENT

TI - Internet protocol address assigning procedure for computer network system, identifies input physical characteristic based on input authentication data upon reception of data through communication unit

PR - JP19990016634 19990126
PN - JP2000216822 A 20000804 DW200108 H04L12/56 007pp
PA - (HITA) HITACHI LTD
IC - G06F13/00 ; G06F15/00 ; H04L12/28 ; H04L12/56

AB - JP2000216822 NOVELTY - The input physical characteristic of a user is identified based on an input authentication data upon reception of data through a communication unit. The communication unit is interconnected to many data processors.

- USE - For computer network system.

- ADVANTAGE - Maintains security when assigning internet protocol address. Ensures reliable assignment of internet protocol address.

- DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of an internet protocol address assigning procedure.

- (Dwg.2/4)

OPD - 1999-01-26
AN - 2001-064719 [08]

© PAJ / JPO

PN - JP2000216822 A 20000804
PD - 2000-08-04
AP - JP19990016634 19990126
IN - ONUMA TETSUYA
PA - HITACHI LTD
TI - METHOD FOR ALLOCATING IP ADDRESS

AB - PROBLEM TO BE SOLVED: To provide a method for allocating an IP address, which can maintain security, by inputting the physical feature of a user and transmitting/receiving inputted certification data as a user identifier through a communication means.

- SOLUTION: When the allocation request of an IP address for accessing a specified segment and a server is generated in an arbitrary terminal machine 20-1, the terminal machine 20-1 inputs a physical feature, a fingerprint, for example, by using a fingerprint certification device 30-1. The fingerprint data is transmitted to a certification server 10 through a public network 70. The certification server 10 executes the collation processing of whether registered data stored in the certification server 10 and the user identifier of fingerprint data are the same or not in accordance with the reception of fingerprint data. When the results of the collation processing are matched, the specified IP address is allocated to a user and the

collation result is-transmitted to the terminal machine 20-1. When the results of the collation-processing are not matched, the allocation of the IP address is judged to be impossible and the effect is transmitted.

I - H04L12/56 ;G06F13/00 ;G06F15/00 ;H04L12/28

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-216822

(P2000-216822A)

(43) 公開日 平成12年8月4日 (2000.8.4)

(51) Int.Cl. ⁷	識別記号	F I	テームコード (参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 D 5 B 0 8 5
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
	15/00		3 3 0 F 5 K 0 3 0
H 0 4 L 12/28	3 3 0	H 0 4 L 11/00	3 1 0 Z 5 K 0 3 3

審査請求 未請求 請求項の数 3 O L (全 7 頁)

(21) 出願番号 特願平11-16634

(22) 出願日 平成11年1月26日 (1999.1.26)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 大沼 哲也

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報システム事業部内

(74) 代理人 100068504

弁理士 小川 勝男

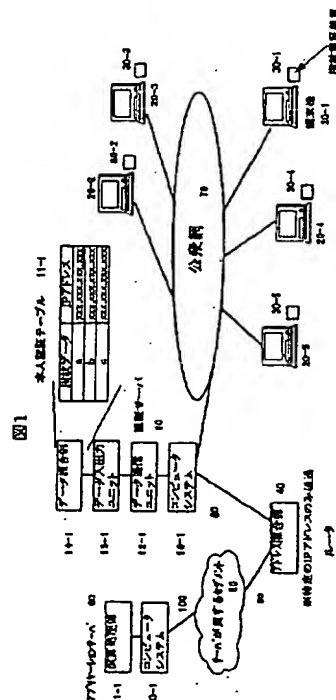
最終頁に続く

(54) 【発明の名称】 IPアドレスの割当て方法

(57) 【要約】

【課題】 外部からリモート・アクセスで使用する場合に、指紋認証を用いることによって「なりすまし」等を防止した特定IPアドレスの割当てができるようにする。

【解決手段】 割当て後、ある一定時間端末機20-1が利用されていない場合、端末機20-1に格納された指紋データと指紋認証装置30-1より入力した照会指紋データを照合し、この照合結果に応じた利用の継続を決定することによって機密保持を維持する。



【特許請求の範囲】

【請求項1】複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段において、利用者の身体的特徴を入力し、入力した認証データを利用者識別子として通信手段を介して送受するコンピュータネットワークシステムを有することを特徴とするIPアドレスの割当て方法。

【請求項2】複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段とを有するコンピュータネットワークシステムにおける特定のIPアドレスの割当て方法であって、利用者の身体的特徴を入力し、入力した認証データを利用者識別子として前記通信手段を介して送受する利用者識別子と照合し、照合結果にしたがって、特定のIPアドレス割当てを決定する方法を有することを特徴とするIPアドレスの割当て方法。

【請求項3】前記特定のIPアドレス割当てを決定する方法は、ある一定時間端末機が利用されていない場合において、利用者の身体的特徴を再問合せし、再入力した認証データを利用者識別子として照合し、照合結果にしたがって、特定のIPアドレス利用の継続を決定する方法を有することを特徴とするIPアドレスの割当て方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、イントラネット上の特定サーバや特定セグメントを外部から利用するために特定IPアドレスを割当てする方法に関し、特に、身体的特徴による本人認証によって本人のみ利用可能にするためのIPアドレスの割当て方法である。

【0002】

【従来の技術】複数のコンピュータシステムを通信網により相互に接続したコンピュータネットワークシステムでは機密保護のため、ネットワークシステムへのアクセス要求に応じて利用者を識別し、それを達成するために特定のIPアドレスを割当て特定のセグメントやサーバにアクセスする処理を行なう必要がある。

【0003】現状、特定のIPアドレスを割当てする方法としては、Macアドレスによって特定の端末に割当てする方法やパスワード入力によって特定の利用者に割当てすることができる。

【0004】

【発明が解決しようとする課題】上述したようなコンピュータネットワークシステムにMacアドレスやパスワード入力による認証を用いてコンピュータシステムまたはネットワークシステムにアクセスを行なう従来の方法では、厳密な機密保護が困難であるという問題点がある。

【0005】従来の特定IPアドレスの割当て方法では、特定の端末機やパスワードを知っている者の利用に対する機密保護については有効である。しかし、本人以

外に利用が認められないケースにおける機密保護については、例えば、パスワードは本当に本人しか知らないのか、あるいは、いわゆる「なりすまし」によって他人が不正に利用していないのか等を確認することが困難である。

【0006】上述の課題から、本発明の目的は、機密保護を維持することが可能なIPアドレスの割当て方法を提供することである。

【0007】

【課題を解決するための手段】この発明に係るコンピュータネットワークシステムにおいて、複数のデータ処理手段は、IPアドレスの割当て要求に対して利用者識別子を送出し、通信手段に接続され、前記通信手段を介して受け取った利用者識別子を、予め登録された利用者識別子と照合し、IPアドレス割当ての可否を判定する照合手段を具備することを特徴とする。

【0008】この発明に係るIPアドレス割当て方法は、複数のデータ処理手段と複数のデータ処理手段を相互接続する通信手段とを有するネットワークシステムにおけるIPアドレス割当て方法であって、割当て要求に応じ、利用者の身体的特徴を入力し、前記認証データを利用者識別子として前記通信手段を介して受信し、照合の結果得られる利用者の特定のIPアドレスを送信することを具備している。

【0009】前記IPアドレス割当て方法は更に、前記通信手段を介して受信される利用者識別子を、予め認証サーバに登録された利用者識別子と照合し、照合結果に従って、特定IPアドレスの割当てを決定することを具備している。

【0010】以上のIPアドレス割当て方法においては、人間の身体的特徴を有する認証データ、本件においては指紋に依存するものであり、各個人に固有のものである。従って、この認証データを利用者識別子として用いてネットワークシステムに対する特定のIPアドレスの割当てを決定すれば、認証データが登録されていない他人による特定セグメントや特定サーバへのアクセスに対して、Macアドレスやパスワード入力による割当てよりも確実な機密保護ができる。

【0011】

【発明の実施の形態】以下、この発明を図面を参照して説明する。図1は、この発明のシステムの概略構成を示すブロック図である。同図に示されるように、複数のコンピュータシステムである認証サーバ10や端末機20-1~20-5が公衆網70を介して相互に接続されている。端末機20-1~20-5には利用者の身体的特徴（認証データ）を入力する指紋認証装置30-1~30-5が各々接続されている。

【0012】前記公衆網70には、端末機20-1より送信された認証データに基づいてコンピュータネットワークシステムに対する利用者が特定セグメントやサーバ

にアクセスすることが可能な特定のIPアドレスを決定する認証サーバ10が接続されている。この認証サーバ10は端末機20-1から公衆網70を介して送られる認証データとこのコンピュータネットワークにおいて予め本人認証テーブル11-1(図3)として登録されている指の特徴データとを照合し、この特徴データと一致した場合、本人認証テーブル11-1に登録されている特定のIPアドレスを割当てる。端末機20-1は、このIPアドレスによって、特定のセグメント50およびアプリケーションサーバ60にアクセスする。

【0013】次に、このコンピュータネットワークシステムにおける端末機20-1および認証サーバ10のIPアドレスの割当て処理を図2のフローチャートに示す。

【0014】コンピュータネットワークシステムにおいて、任意の端末機20-1で特定のセグメントおよびサーバをアクセスするためのIPアドレスの割当て要求が発生すると、この端末機20-1では指紋認証装置30-1を用いて身体的特徴、本件においては指の指紋を入力する(201)。この指紋データを、公衆網70を介して認証サーバ10に送出される(202)。

【0015】認証サーバ10では、指紋データの受信に応じ、認証サーバ10に格納されている登録データと、前記指紋データの利用者識別子が同一であるか照合処理が行なわれる(203、204)。照合処理の結果が一致である場合、利用者に対し、特定のIPアドレスが割当てられ、照合結果を端末機20-1に送信される(205、206)。一致しない場合は、IPアドレス割当て不可と判断され、この旨が送信される(207、208)。

【0016】その後、端末機20-1では割当て結果を端末利用者に表示する(209)。さらに、IPアドレスが通知されたかを確認し、アドレスが割当てられた場合には端末機20-1に登録され、指紋データも格納される(210、211)。

【0017】次に、端末機20-1に特定IPアドレスを割当てた後の継続利用処理を図4のフローチャートに示す。ある一定時間端末機20-1が利用されていない場合、端末機20-1は利用者に対し、身体的特徴の照合を要求する(401)。利用者は再度、指紋認証装置30-1を用いて身体的特徴を入力する(402)。指紋認証装置30-1より照合指紋データを転送された端末機20-1は、IPアドレス割当て時に格納した指紋データと照合する(403、404)。データが一致した場合には、端末機20-1のネットワークシステム上での利用が継続して利用できる(405)。データが一致しない場合には、照合指紋データを認証サーバ10に送信する(406)。

【0018】認証サーバ10では、照合指紋データと登録データを照合する(407、408)。データが一致

しない場合には、端末機20-1に登録されていたIPアドレスを消去し、ネットワークシステムのコネクションが切断される(409、410)。データが一致した場合には、認証サーバ10の登録データを端末機20-1に送信される(411)。

【0019】端末機20-1では、登録データが通知された場合、指紋データを更新する(412、413)。

【0020】以上説明したように、この方法によれば人間の身体的特徴を示すデータを利用者識別子となる認証データとして、予め登録されている登録データと比較照合することでネットワークシステムにおける特定のIPアドレスの割当ての可否が決定される。さらに、利用者の利用が中断した場合に、身体的特徴を示すデータを用いた再照会におけるIPアドレスの継続利用の可否が決定される。

【0021】これにより、登録データに登録されていない他人によるアクセスに対してMacアドレスやパスワード入力による特定IPアドレスの割当てよりも確実な機密保護を実現できる。

【0022】

【発明の効果】以上詳述したように、この発明によれば、コンピュータシステムにおいて身体的特徴データを用いたIPアドレスの割当てにより、例えばイントラネットを利用する外部利用者からの利用要求に対するIPアドレス割当てが、確実に機密保護を維持することが可能となる。

【0023】特に、人間の身体的特徴を示す特徴を抽出して得られる認証データを利用者識別子として、予め登録されている登録データと比較照合することでネットワークシステムに接続する端末機に対する特定のIPアドレス割当ての可否が決定される。これにより、登録データが登録されていない他人によるイントラネットのアクセスに対して、Macアドレスやパスワード入力によるIPアドレスの割当てを用いてアクセスするよりも確実な機密保護を実現できる。

【図面の簡単な説明】

【図1】本発明の実施例におけるシステム構成を示すブロック図。

【図2】本発明の実施例におけるIPアドレス割当て処理を示すフローチャート。

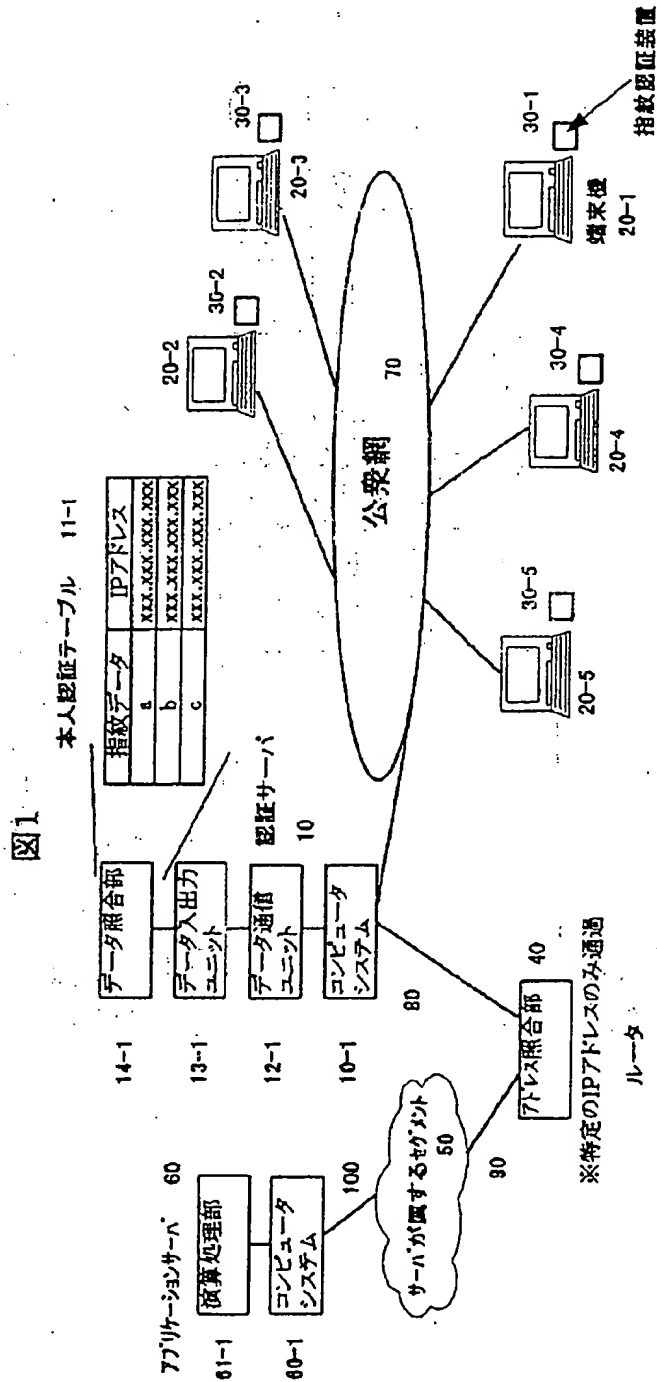
【図3】本発明の実施例における本人認証テーブルを示す図。

【図4】本発明の実施例における継続利用処理を示すフローチャート。

【符号の説明】

10…認証サーバ、20-1～4…端末機、30-1～4…指紋認識装置、40…ルータ、50…サーバが属するセグメント、60…アプリケーションサーバ、70…公衆網、80、90、100…通信回線、11-1…本人認証テーブル。

【図1】

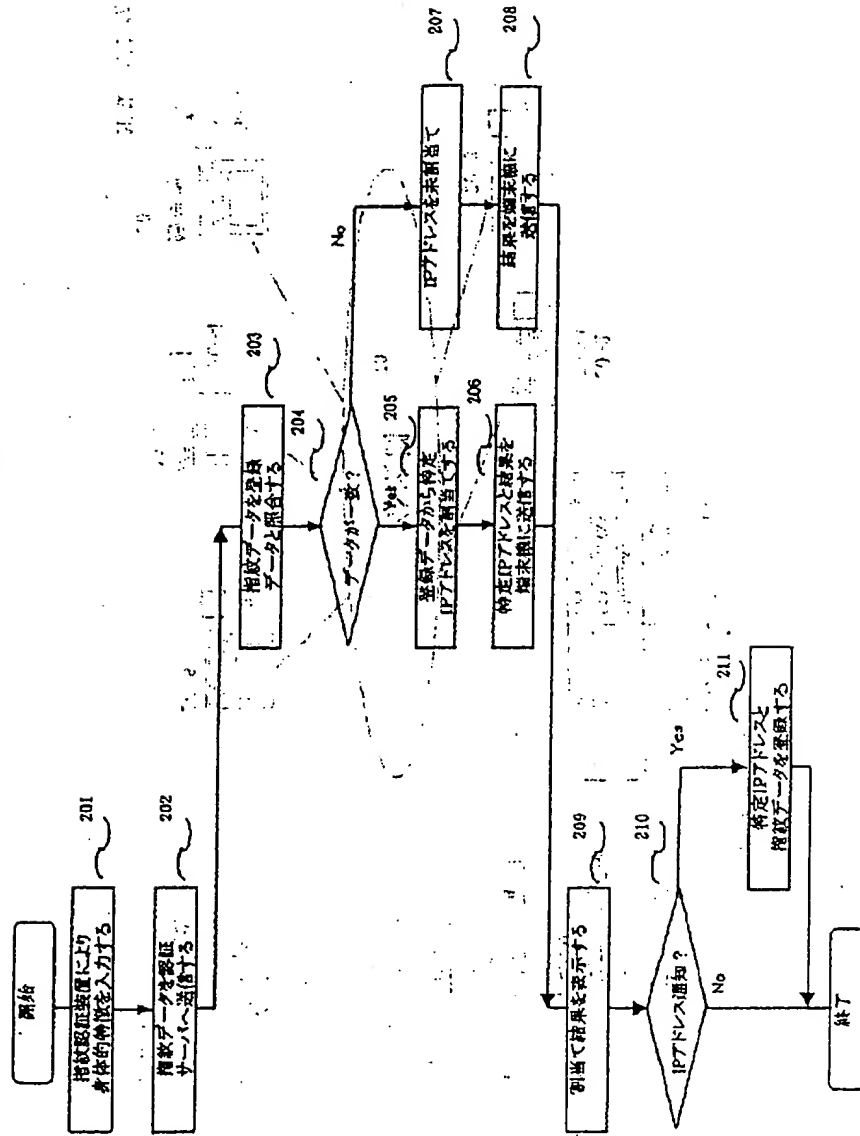


【図2】

図2

端末の処理

認証サーバの処理



【図3】

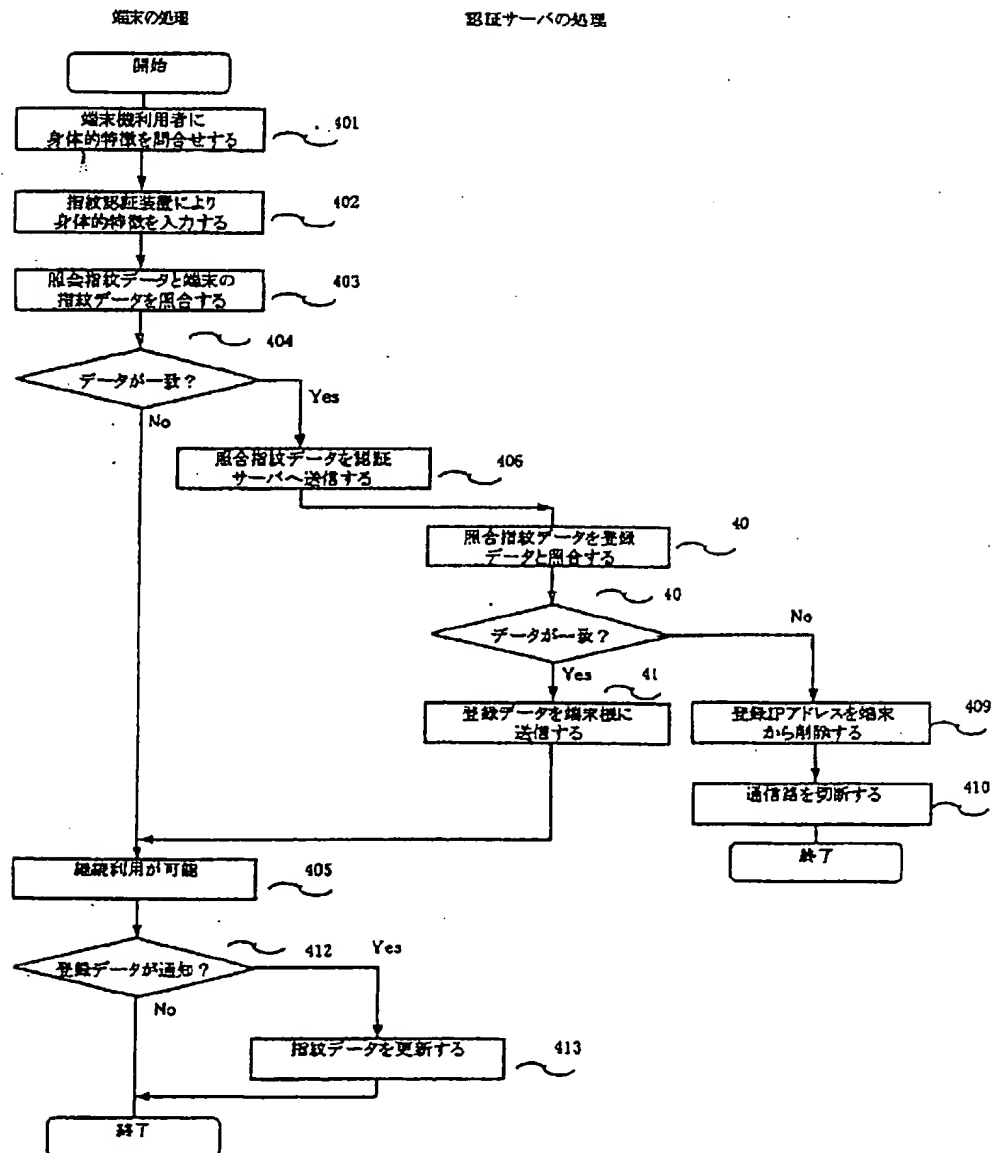
図3

指紋データ	IPアドレス
a	XXX.XXX.XXX.XXX
b	XXX.XXX.XXX.XXX
c	XXX.XXX.XXX.XXX

※テーブル中のIPアドレスは各1で全てユニーク

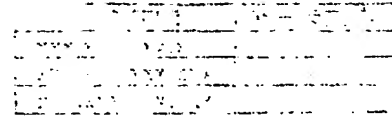
【図4】

図4



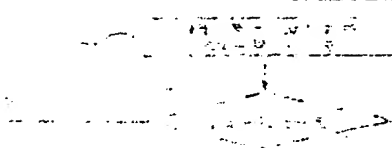
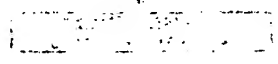
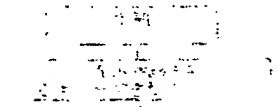
フロントページの続き

Fターム(参考) 5B085 AE23 AE26 BG07
5B089 GA21 GB01 HA10 JB22 KA17
KB06 KB13 KC29 KC47 KC58
LB10
5K030 GA15 HA08 HC01 HC14 HD06
HD09 LD18 LD20
5K033 AA08 BA04 CB08 DA06 EC03



[1]

2000-2158



2000-2158

